IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE GOOGLE INC. ACCOUNT PERS4LISA@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE INC. 1600 AMPHITHEATRE PARKWAY MOUNTAIN VIEW, CA 94043	))))))))	MAG 17-23

MEMORANDUM OPINION and ORDER

The government has applied to the court for the issuance of a search warrant to obtain the contents of and information related to a certain email account. Although the court finds probable cause to issue the warrant, the court has great concerns about various aspects of the search warrant, including the scope and magnitude of the information it seeks, whether it particularly describes the things to be seized, and how the search and seizure of information in electronic files take place. This Order not only attempts to explain the court's concerns, but also to put in place mechanisms for reducing what the court views as a tension between the nature of electronic searches and the Fourth Amendment.

I. Background

The search warrant application relates to an investigation into possible wire and bank frauds. The details of the investigation are not important to the search warrant issues addressed in this Order other than to say that the application adequately showed probable cause to search for and seize information from the named email account. After the application described the investigative facts relied upon to establish probable cause, the warrant application requested authority to require a third-party internet service provider to produce to the government certain

items described in an attachment to the application. In Section I of Attachment B, the warrant requires the internet service provider to produce the following to the government:

> A. From January 1, 2012, to December 31, 2016, the full content of Google Mail, including the contents of all emails associated with the account, including any stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the email;
>
> B. From January 1, 2012, to December 31, 2016, the contents of all chat messages and logs associated with the account, including stored chat messages and logs;
>
> C. The contents of all SMS messages and logs associated with the account, including stored SMS messages and logs;
>
> D. The files and contents associated with the account related to Google services such as Google Drive, Google Docs, Google search history, Google bookmarks, Google Picasa files, Google play purchases, Google Sites, Google voice and voicemail, Google wallet, Google +, Google Orkut, and YouTube videos;
>
> E. All records or other information regarding the identity of the account holder, including full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
>
> F. The types of service utilized, including the names of any other accounts associated with this account;
>
> G. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
>
> H. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

I. Any and all embedded metadata, such as header information, creation dates, and GPS location data, associated with any of the items produced in compliance with this warrant;

J. Any and all methods of payment provided by the subscriber to the Provider, Inc. for any premium services, including account numbers; and

K. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored. The Provider is hereby ordered to disclose the above information to the government within fourteen days of the issuance of this warrant.

Upon the production of this information from the internet service provider, the government proposes to seize, the following:

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Section 1030 (fraud and related activity in connection with computers), Section 1341 (mail fraud), Section 1343 (wire fraud), Section 1344 (bank fraud), and Section 371 (conspiracy to commit the above-described offenses), including the following:

A. Records of any communications between pers4lisa@gmail.com and any other party relating in any way to the crimes specified in the introductory paragraph above;

B. Records indicating the identity of the person(s) who created or used the pers4lisa@gmail.com, including records that help reveal the whereabouts of such person(s);

C. Evidence indicating how and when the email account pers4lisa@gmail.com was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

D. Evidence indicating the email account owner's state of mind as it relates to the crimes under investigation;

E. Records indicating the identity of the person(s) who communicated with the email address pers4lisa@gmail.com about matters relating to checks, wires or financial transfers, banking transactions, or the use of encrypted communication technology, including records that help reveal their whereabouts; and

F. Records indicating the identities of co-conspirators, accomplices, and aiders and abettors in the commission of the above offenses.

The government's procedures for sifting through the materials produced by the internet service provider to identify and segregate the categories of information to be seized by the government are not described in the application, but the court suggested to the lawyer for the government that using a "filter team"[1] is necessary to preserve any legitimate privacy interest in any non-criminal contents of the account.

II. The Applicable Law

The warrant application invokes 18 U.S.C. §§ 2703(a), (b)(1)(A) and (c)(1)(A) for its foundational authority, but these provisions do nothing more than require the use of a search warrant to obtain the types of electronic information being sought. Accordingly, the court refers to Fed. R. Crim. P. 41 for guidance, illuminated, of course, by the fundamental constitutional requirements of the Fourth Amendment.

For issuing a search warrant, Rule 41(e)(2)(A) mandates that the warrant "must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned." Specifically for searches of electronically stored information, Rule 41(e)(2)(B) requires:

---

[1] The term "filter team," also sometimes referred to as a "taint team," is meant to describe a procedure under which a group of lawyers and/or agents not directly involved in the investigation conducts the sifting search of the materials produced by the internet service providers, rather than the search being conducted by the lawyers and agents directly involved in the investigation. The filter team identifies and segregates the information coming within the scope of the warrant, while keeping separate from the investigating lawyers and agents the remaining information produced but not within the scope of the warrant. The purpose of a filter team is to allow the government to execute the search warrant while preserving the privacy of irrelevant information from the prosecution team.

> (B) *Warrant Seeking Electronically Stored Information.* A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

Furthermore, an inventory of items seized must be maintained by the executing officer, but

> In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

Fed. R. Crim. P. 41(f)(1)(B). Finally, upon the seizure of property – presumably including electronically stored information – a person affected by the seizure may move for return of the property. Rule 41(g) states:

> (g) *Motion to Return Property.* A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

The procedures described in Rule 41 all must be construed against the backdrop of the constitutional protections of the Fourth Amendment. Certainly, neither Rule 41 itself nor any statute may dispense with a constitutional requirement under the Fourth Amendment. The Fourth Amendment protects not just people and places, but the inherent privacy one often expects in communications and information. For example:

> The Fourth Amendment, as applied to the states by way of the Fourteenth Amendment, see Mapp v. Ohio, 367 U.S. 643, 646–47, 81 S. Ct. 1684, 6 L. Ed. 2d 1081 (1961), protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. For our purposes, a Fourth Amendment search occurs "when the government violates a subjective expectation of privacy that society recognizes as reasonable." Kyllo v. United States, 533 U.S. 27, 33, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001).
>
> Almost 50 years ago, the Supreme Court held that a "'conversation [is] within the Fourth Amendment's protections," and that "the use of electronic devices to capture it [is] a 'search' within the meaning of the Amendment." See Berger v. New York, 388 U.S. 41, 51, 87 S. Ct. 1873, 18 L.Ed.2d 1040 (1967) (invalidating a New York statute that authorized the electronic interception of private conversations by the police (through recording devices installed in various offices) pursuant to a court order, on the ground that the procedures for obtaining the order were insufficient to comply with the Warrants Clause of the Fourth Amendment).

Gennusa v. Canova, ___ F.3d ___, 2014 WL 1363541, *3 (11th Cir., Apr. 8, 2014). To preserve this reasonable expectation of privacy, the Fourth Amendment authorizes searches only upon a showing of probable cause to a detached and neutral magistrate that there is a "fair probability" that specified contraband or fruits or evidence of crime can be located in a particular place. United States v. Jiminez, 224 F.3d 1243, 1248 (11th Cir. 2000) (quoting Illinois v. Gates, 462 U.S. 213, 238, 103 S. Ct. 2317, 2332, 76 L. Ed. 2d 527 (1983)); see also United States v. Bradley, 644 F.3d 1213, 1259 (11th Cir. 2011).

An important element of this constitutional requirement is that the warrant describe with particularity not only the place to be searched, but also the thing or things to be seized. The specificity requirement has two parts:

> "'In order for a search to be reasonable, the warrant must be specific. Specificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based.'" United States v. Maali, 346 F.Supp.2d 1226, 1239 (M.D.Fla. 2004)

> (quoting In re Grand Jury Subpoenas Dated December 10, 1987, 926 F.2d 847, 856–57 (9th Cir. 1991))..... "'The scope of the warrant, and the search, is limited by the extent of probable cause.... [P]robable cause must exist to seize all items of a particular type described in the warrant' and '[t]hus, the concept of breadth may be defined as the requirement that there be probable cause to seize the particular thing named in the warrant.'" Id. (citation omitted); see also United States v. Smith, 424 F.3d 992, 1004 (9th Cir. 2005) ("The purpose of the breadth requirement is to limit the scope of the warrant 'by the probable cause on which the warrant is based.'") (citation omitted). The breadth requirement, therefore, prevents "'general, exploratory rummaging in a person's belongings.'" Smith, 424 F.3d at 1004 (citation omitted).

United States v. Lebowitz, 647 F. Supp. 2d 1336, 1351 (N.D. Ga. 2009) aff'd, 676 F.3d 1000 (11th Cir. 2012). The Supreme Court also has linked the particularity requirement to prevention of general exploratory searches, saying:

> The Warrant Clause of the Fourth Amendment categorically prohibits the issuance of any warrant except one "particularly describing the place to be searched and the persons or things to be seized." The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit. Thus, the scope of a lawful search is "defined by the object of the search and the places in which there is probable cause to believe that it may be found. Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase." United States v. Ross, 456 U.S. 798, 824, 102 S. Ct. 2157, 2172, 72 L. Ed. 2d 572 (1982).

Maryland v. Garrison, 480 U.S. 79, 84-85, 107 S. Ct. 1013, 1016-17, 94 L. Ed. 2d 72 (1987); see also Coolidge v. New Hampshire, 403 U.S. 443, 467, 91 S. Ct. 2022, 2038, 29 L. Ed. 2d 564 (1971); United States v. Bradley, 644 F.3d 1213, 1259 (11th Cir. 2011). "'The description is considered sufficiently particular when it enables the searcher to reasonably ascertain and identify the things authorized to be seized.'" United States v. Bradley, 644 F.3d 1213, 1259

(11th Cir. 2011) (quoting United States v. Betancourt, 734 F.2d 750, 754 (11th Cir.1984)). "This requirement does not necessitate technical perfection; instead, it is applied with 'a practical margin of flexibility.'" Id. (quoting United States v. Wuagneux, 683 F.2d 1343, 1349 (11th Cir.1982)).

III. The Warrant in Question

The court concluded that the search warrant application established probable cause to search for certain information in the subject email account. Based on the application, there is a "fair probability" that evidence of federal crimes will be found in the account. But it is also true that, in seizing *all* of the contents of the accounts over a five-year period, it is likely that materials and information utterly unrelated to the offenses under investigation will be seized along with the potentially incriminating evidence. The question troubling the court is, how can the warrant be executed in a way that allows the government to obtain the criminal evidence it seeks without unconstitutionally invading the privacy interests of the account holder in materials and information not relevant to the investigation?

Under the procedures described in the warrant application, the internet service provider will copy and produce to the government on some electronic medium (probably a disk) all information related to the identified email account between certain dates. The court is persuaded that this procedure of sweeping up the entire contents of an email account for review at the later time is consistent with both Rule 41 and the Fourth Amendment because there is no practical alternative. Rule 41 explicitly authorizes a warrant to allow for "copying of electronically stored information.... [with] a later review of the media or information consistent with the warrant." The alternatives to obtaining a copy of the requested electronically stored information is to conduct the search directly on the internet service provider's server or to request that the internet

service provider conduct the search by some means such as key-word searching. The former is not practical and the latter is not required by the Fourth Amendment. Searching through massive amounts of electronically stored data, with the requisite examination of each data file, often can take hours or days, during which time the server containing the information is not available for use by the internet service provider. Not only does this burden the third-party owner of the server, it does not eliminate the potential Fourth Amendment objection that government agents had to examine each and every data file, including the irrelevant ones, to identify and copy only those within the scope of the warrant. Searching for needles in a digital haystack still requires examination of most if not all of the digital hay. As to requiring the internet service provider itself to conduct the search, this requires the agreement of a third-party to expend its time and resources to conduct the search for the government, while depriving the government of its authority to execute the warrant. The government generally is not required to turn over the execution of a search warrant to a private entity.

In the domain of warrants issued for electronically stored information, traditional notions of when a "search" occurs and when a "seizure" occurs are not as simple as in the physical world. The interests protected by the Fourth Amendment are different for searches than for seizures. The Supreme Court has explained on more than one occasion that

> The first clause of the Fourth Amendment provides that the "right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated...." This text protects two types of expectations, one involving "searches," the other "seizures." A "search" occurs when an expectation of privacy that society is prepared to consider reasonable is infringed. A "seizure" of property occurs when there is some meaningful interference with an individual's possessory interests in that property.

United States v. Jacobsen, 466 U.S. 109, 113, 104 S. Ct. 1652, 1656, 80 L. Ed. 2d 85 (1984) (internal footnotes omitted); see also Horton v. California, 496 U.S. 128, 133-34, 110 S. Ct. 2301, 2306, 110 L. Ed. 2d 112 (1990) ("A search compromises the individual interest in privacy; a seizure deprives the individual of dominion over his or her person or property."). Thus, the seizure of an item in plain view compromises the possessory interests of the owner of the item but does not invade any expectation of privacy. See Horton at 134.

In the cyber-world of electronically stored information, these privacy and possessory interests must be measured against the *information* or *data*, not simply the physical media on which the information or data are stored. For example, when an internet service provider copies digital data to a disk and delivers the disk to the government, has any *privacy* interest or *possessory* interest been invaded or compromised? Certainly, until some government agent *accesses* and *reads* the electronically stored information on the disk, no *privacy* interest has been invaded. The physical disk itself reveals nothing about the data on it, just as a closed package reveals nothing about the contents of the package. If the data on the disk are never accessed, no privacy is lost. See generally Orin Kerr, Searches and Seizures in a Digital World, 119 Harv. L.Rev. 531, 551 (2005) (search does not occur until "the data is exposed to possible human observation").

Whether a "seizure" has occurred is more problematic. Plainly, the owner of an email account has no *possessory* interest in either the server of the internet service provider or the physical disk to which information might be copied. Does the *copying* of the digital data itself interfere with the "dominion" of the account owner over the information copied? Even after ESI is copied, the account owner can still access his own account and the information in it; he is not

deprived of the use of the data.[2] The account owner *is* deprived of his control over to whom the electronically stored information is shared, and while this looks more like a question of privacy rather than possessory dominion, as explained below, it is both.

It might be argued that a "seizure" of electronically stored information occurs only when the information is *used* in some fashion; only then has the owner's dominion over the information been compromised. Unlike physical objects, the mere possession of which amounts to control, control and dominion over *information* can be understood only in terms of by whom and under what circumstances it can be *used.* Mere possession of information creates no dominion over it for, unlike a physical object, information can be simultaneously "possessed" by more than one person, each of whom may have different degrees of control over its use.[3] In a sense, therefore, privacy interests and possessory interests in information merge – the only way to maintain a possessory interest in information is to keep it private. Only by controlling who has access to information can the owner of the information protect both his privacy interest in it *and* his control (or dominion) over its use.

Taking this approach, the court believes that a Fourth Amendment "seizure" of electronically stored information occurs only when the information is accessed by investigating agents and a determination is made that it is within the scope of the warrant. Only at that point

---

[2] This illustrates how electronically stored information is fundamentally different from information stored in paper or physical files, which can be seized, depriving the owner of access to their use.

[3] But see Matter of the Search of Info. Associated with [redacted]@mac.comthat is Stored at Premises Controlled by Apple, Inc., 14-228 (JMF), 2014 WL 945563 at *5 (D.D.C. Mar. 7, 2014), reasoning that mere delivery of copied digital data to the government means that "the seizure of a potentially massive amount of data without probable cause has still occurred—and the end result is that the government has in its possession information to which it has no right."

in time has the information owner's privacy in it been invaded and his ability to control its use – his dominion over it – has been compromised. If the data disk is never accessed and later destroyed, neither privacy nor possessory control over the use of the *information* on the disk has been invaded. If the information on the disk is accessed by an investigating agent, both a "search" (i.e., invasion of a privacy interest) and a "seizure" (i.e., interference with dominion over the information) occurs.

As stated earlier, it is likely that the email information sought in this warrant will include a significant amount of information unrelated to the criminal investigation and, thus, beyond, the scope of the warrant.[4] The court recognizes that application of the particularity requirement must be "flexible" and not "overly elaborate," United States v. Bradley, 644 F.3d 1213, 1259 (11th Cir. 2011). Nevertheless, to avoid overbreadth, the description of things to be seized must be supported by probable cause. Due to the nature of the information in email accounts, it is likely that a significant portion of the electronically stored information produced in response to this search warrant will not be supported by probable cause. To protect the account owner's expectation of privacy in such non-relevant information, the government must take steps to prevent the undue intrusion on electronically stored information not reasonably probative of the offenses described in the warrant. It is the alleged commission of these offenses that justifies the

[4] The government makes the argument that electronically stored information in the email accounts is relevant even if not directly probative the criminal offense, because such other information tends to prove the identity of the person actually utilizing the email account. The government analogizes it to seizing utility statements and letters during the search of a house as proof of who resides there. The court believes this stretches the particularity requirement beyond the breaking point. In essence the government contends that *everything* in the email account is relevant as potential evidence of the use of the account. This position, however, eviscerates the particularity requirement by attaching some theoretical or hypothetical evidentiary value to everything. No longer would there be a need to describe with particularity the things being sought because *everything* is being sought. The court does not believe this comports with the particularity requirement of the Fourth Amendment.

intrusion in the first place, and thus the scope of the intrusion on privacy must be limited to the evidence reasonably identifiable as relevant to investigation and prosecution of the named offenses. Therefore, this Order is entered with respect to execution of the warrant described above to provide for a protocol for protecting the privacy of non-evidentiary materials produced by the internet service providers in response to the warrant.

It is therefore ORDERED, that, upon production of the electronic information relating to the subject email account, the government shall use a filter team, separate and apart from the investigative/prosecutorial team, to identify and extract that electronic information relevant to the offenses under investigation. Upon completion of the review by the filter team, it shall turn over to the investigative/prosecutorial team the electronically stored information that the filter team reasonably identifies as being within the scope of these warrants due to the information's evidentiary value directly probative of the offenses described in the warrant application. The filter team shall not disclose to the investigative/prosecutorial team any other non-relevant information produced by the internet service provider. The government shall then SEAL and maintain possession of the *remaining* electronically stored information, which shall not be accessible to the government except upon the granting of another search warrant or further Order of the court. It is the intention of this Order to allow the government to extract and use that electronically stored information directly probative of the offenses described in the warrant application, while sealing the remainder of the information produced from further intrusion by the government without a new warrant or court order.

The Clerk is DIRECTED to SEAL this Order along with the warrants and warrant applications, but to mail a copy of the Order to the United States.

DONE this 6th day of February, 2017.

T. MICHAEL PUTNAM
UNITED STATES MAGISTRATE JUDGE